

SYSTEM CONSOLE DEVICE AUTHENTICATION IN A NETWORK ENVIRONMENT

BACKGROUND OF THE INVENTION

1. Technical Field:

The present invention relates in general to computer system and in particular to accessing console features of a networked computer system. Still more particularly, the present invention relates to a method and system for improved security access for console devices and/or console device features of a networked computer system.

2. Description of the Related Art:

Computer networks or multi-user computer systems are common in today's business environment and may range from small, localized, local area networks (LANs) to larger, geographically, dispersed wide area networks (WANs), such as the Internet. Irrespective of the type and size of network, the network setup, control, and maintenance are usually performed by operators or administrators having specialized access and utilizing specialized console devices.

Multi-user computer systems typically support a system console mode of operation that is used by the system administrator to setup and manage the computer system. System administrator functions include installing software applications, installing software updates (and fixes), performing file backup and restore operations, managing security controls, and giving new users access to applications and system resources. The console mode of operation runs either separately (in the case of initial setup) or concurrently with user applications. The console mode of operation can also

be utilized by service personnel to perform service functions and problem determination.

Typically, console functions are restricted to designated console operators. The restriction to designated operators provides added security to the computer system and ensures the integrity of the system. Access to the console operations is controlled by the "system console control program", which authenticates a console operator. The operator is required to enter a user-identifier (user ID) and his/her associated password.

Typically, to ensure added security and integrity, console functions are allowed and supported only on particular devices (e.g., keyboard/display terminals or workstations) that may be located in a protected, controlled physical environment. These console devices have simple command line and/or text menu interfaces because of the limited resources of the system console control program during early phases of system initialization and setup and when performing service functions. For example, iSeries™ console devices connect to the system via a twinaxial serial port or an asynchronous RS-232 serial port. These types of connectivity also require the console device to be in close physical proximity to the system. Additionally, some systems (e.g., iSeries™) support multiple-logical system partitions, where each partition requires its own console device.

Present mechanisms used to protect console functions do not identify and authenticate the device from which the console function request is being made. These other mechanisms rely upon physical controls such as special connectivity (i.e., a special communication cable, such as a TWINAX connection) or special physical device controls (i.e. the device accessing the console functions has to be located in a secure room in close physical proximity to the system) or an identity scheme based on

the unique burned-in identifier in the console device's network adapter card (which can be shared among systems and is not secure). These restrictions in present mechanisms limit the capabilities of allowing access to the console functions and thus reduce the security, usability, and functionality of the system.

5

With the widespread use of LANs, there is a growing need to provide more flexibility in attaching and supporting console devices in a networked environment. Thus, system administrators do not want specialized devices, which require special communications ports (with corresponding cable length restrictions) to perform system console functions. Instead, system administrators want to utilize LAN-attached PCs or, in the more general case, network-attached devices to provide console support.

10

Providing console support on network-attached devices enables a wider selection in the types of devices that may be utilized and allows greater flexibility in the physical placement or location of the device. Also, network-attached devices (in the case of personal computers) are capable of running multiple console sessions (e.g., one session for each system in the network or for each logical partition in a system). However, capitalizing on the flexibility of allowing console operations from any network-attached device exposes potentially serious security issues, including:

15

20

a. restricting console functions to a particular device (i.e., a system administrator may still require that a console device be located at a particular location on the physical premises);

b. passing a user-id and associated user-id password to authenticate the console operator over an insecure network;

25

c. console session data passing across an insecure network un-encrypted and available to be viewed by unauthorized persons; and

d. ensuring that the integrity of the console session data is maintained (i.e., not modified) when flowing across the network.

There are some user-authentication methods being presently utilized such as described in U.S. Patent No. 5,434,918. However, these methods focus specifically on user-to-server authentication and do not provide any solution to issues of continuing console device authentication and preserving data integrity during console operations.

The present invention thus recognizes that it would be desirable to provide a method and system for enhancing security of access to console operations from network-attached console devices. The invention recognizes that it would be desirable to enable authentication of a device to be utilized as a console device. The invention further recognizes that it would be desirable to enable secure transmission of console functions and/or sessions data to and from a network-attached device. These and other benefits are provided in the present invention.

SUMMARY OF THE INVENTION

A method for providing secure access to console functions of a computer system and authentication of a console device is disclosed. The method comprises first initiating a first Encrypted Key Exchange (EKE) sequence to generate a unique shared secret per device utilizing a default device identifier and associated default shared secret on a system-attached device from which a console operation is desired to be enabled. Then, a shared secret is generated from the first EKE sequence, and the generated shared secret is utilized in place of the default device shared secret in subsequent console authentication procedures for that device. Following, the shared secret is securely stored within a storage location of the system and on the system-attached device. The device's shared secret is subsequently replaced for each connection from that device.

The shared secret is stored in a protected manner on the system-attached device and utilized as the device shared secret during each connection of said system-attached device to said system. Following the first EKE sequence, operator authentication data flowing between said system-attached device and the system are encrypted utilizing the shared secret.

When the first console session is established and the system-attached device is authenticated, then a second EKE sequence is initiated to authenticate a console operator utilizing a default user identifier and password. The user identifier and password are stored in a protected area of said storage location of said system and are not stored on the system-attached device.

In operation, multiple device identifiers and associated shared secrets and authorization levels for other system-attached devices to act as console devices may

be implemented. The multiple device identifiers and authorization levels are stored in a special secure system storage location. Additionally, multiple operator user identifiers and associated passwords and authorization levels for other console operators to access console functions of the system may be established. These multiple operator user identifiers and associated passwords and authorization levels are also stored in a special secure storage location. Thus multiple console sessions for different systems are enabled on a single console device. Also, each console device may be a console for multiple machines, each server may have multiple connected console devices, and each console device may have multiple users.

The invention accomplishes four major goals: (1) restricting console function to a particular device via device authentication; (2) securely passing a user-id and associated user-id password to authenticate the console operator; (3) protecting console session data from being viewed by unauthorized persons; and (4) ensuring that the integrity of the console session data is maintained (i.e., not modified) when flowing across the network.

The above as well as additional objects, features, and advantages of the present invention will become apparent in the following detailed written description.

BRIEF DESCRIPTION OF THE DRAWINGS

The novel features believed characteristic of the invention are set forth in the appended claims. The invention itself however, as well as a preferred mode of use, further objects and advantages thereof, will best be understood by reference to the following detailed description of an illustrative embodiment when read in conjunction with the accompanying drawings, wherein:

Figure 1 depicts a block diagram of major components of a data processing system, in which a preferred embodiment of the present invention may be implemented;

Figure 2 depicts a network with attached console devices within which a preferred embodiment of the present invention may be implemented;

Figures 3A-3D illustrate a series of authentication procedures between a network-attached console device and system server in accordance with a preferred implementation of the present invention;

Figures 4A and 4B are high level logical flow charts depicting the processes of providing access authentication in accordance with preferred implementations of the present invention; and

Figures 5A and 5B illustrate high level block diagrams of a client and server device configuration in accordance with one embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention is directed to a method and system for providing secured authentication for access to console operations on a network via network-attached devices utilized as console devices. The network-attached device may be a standard data processing system as illustrated in **Figure 1**, and the network may comprise server-connected devices as provided in **Figure 2**. The invention may, however, be implemented in other types of data processing systems and network configurations and, while the present invention may be described with reference to the provided figures, these references should not be construed in a limiting sense.

The present invention makes use of the encrypted key exchange (EKE) algorithm described in United States Patent (Ser. No. 5,241,299) entitled "Cryptographic Protocol For Secure Communications," the relevant content of which is hereby incorporated by reference. It is to be understood, however, that the invention may be implemented with other similar encryption algorithms including algorithms yet-to-be developed that utilize the basic framework or functionality of the EKE algorithm, and the references herein to a specific EKE algorithm should not be construed as limiting the invention to only that algorithm.

With reference now to the figures and in particular with reference to **Figure 1**, a high level block diagram of the major component parts of a data processing system that may be utilized as a network-attached device (or console device) or a network server is presented. Data processing system **100** comprises a Central Processing Unit (CPU) **101**. CPU **101** is coupled to system memory **103**, which may be a flash memory in some devices, peripheral input/output (I/O) devices **105**, firmware **111**, and temporary memory **107** via interconnect **109**. Stored within memory devices are the operating system (OS) and software code or logic by which many of the processes

of the invention (e.g., authentication via EKE encryption) may be completed may be implemented as will become clear later. During operation, the software code or logic is executed by CPU **101** in system memory **103** utilizing operator-inputted data (e.g., device ID, device shared secret, and user authentication ID, etc.) The operator
5 interfaces with data processing system **100** (and network) via I/O devices **105**.

Among the I/O devices connected to the CPU may be keyboard, mouse, CD ROM, and display monitor. A display monitor provides a graphical user interface (GUI), which allows a user to view and interact with the console authentication
10 software applications stored in system memory or provided via a network, by displaying icons or other selectable mechanisms with which the user may interact.

Also coupled to CPU are various external devices (not shown). These external devices may include a modem and/or a network adapter utilized to connect data processing system **100** to other systems and/or networks, as is illustrated in
15 **Figure 2**.

In one embodiment a modem may be utilized to connect data processing system **100** to a network server via remote access protocols. In yet another
20 embodiment, a network adapter is utilized to connect data processing system **20** to a Local Area Network (LAN) as depicted in **Figure 2**.

Referring now to **Figure 2**, a high-level block diagram of a server-client based network is illustrated in accordance with a preferred embodiment of the present
25 invention. The network may consist of a single server or a number of servers and provides network clients with a means of communicating and transferring software and information electronically within the network environment.

The preferred embodiment of the present invention is concerned with the controlling of access to system console functions on a network using an authentication procedure that not only authenticates the operator each time he/she accesses the console program and the device but also encodes data transmitted during the console session to prevent unauthorized access or interception. As illustrated, network **200** comprises a computer system (or server) **203** that includes console control program **204A**, device table **204B**, and user table **204C**. Application of device table **204B** and user table **204C** are described further below. Connected to server **203** are three client systems **207A-207C**. Client systems **207A-207C** comprise data processing system **100** illustrated in **Figure 1**, and may each be utilized as a system console device in the present invention. Client system A **207A** is directly connected to server **203** via local connection **209**. Client systems **207B**, **207C** are connected to server **203** via a network **205**, which may be a LAN or WAN. Connection between server **203** and client systems **207B**, **207C** may be via direct access (e.g., an ethernet with connection lines) or remote access (e.g., wireless access).

As illustrated, client system A **207A** includes a hard drive on which is stored the device ID and associated shared secret utilized by the authentication process described below. Client system B **207B** stores the device ID and associated shared secret in a security chip on the system board of the data processing system, while client system C **207C** stores its device ID and associated shared secret in a smart card. Illustration of the various storage areas of the device ID and associated shared secret is meant only to indicate some of the possible storage locations and not meant to be exhaustive of the possible storage locations.

Network server **203** in the present embodiment is a data processing systems having a database, OS, and server software. The preferred embodiment is

implemented with an iSeries server manufactured by International Business Machines, Inc. Each client system is also a data processing system with OS and client software stored locally in memory. Client systems being utilized as console devices also have console device activation software to support sign-in authentication procedures. Client systems utilized as console devices have input mechanisms and visual output mechanism, such as a monitor, by which a system administrator may manage the network. Those skilled in the art appreciate that the network as illustrated herein is a basic network and that even more complex networks, such as those with multiple servers and large numbers of client systems (and/or console devices) and multiple interconnecting networks are contemplated within the scope of this invention.

The invention consists of three main functional elements, which, when combined, provide system administrators with the ability to control and restrict access to console operations to specific devices and operators in a networked environment, such as illustrated in **Figure 2**, when operating in either a limited functional environment or a fully functional environment. Accordingly, in the preferred embodiment, only an authorized and authenticated device and an authorized and authenticated operator are provided access to console operations in the networked environment.

Figures 3A-3D illustrates a series of information blocks within the authentication procedure of the invention, which is described below with reference to the flow charts of **Figures 4A** and **4B**. Directional arrows in **Figures 3A-3D** indicate the exchange of information between the console device and the system as the authentication procedure and later transfer of session data occurs.

Figure 4A is a flow chart illustrating the process of establishing and implementing a secured authentication procedure according to the present invention. The process begins at block **401** and thereafter proceeds to block **403** where default values for the device identifier, shared secrets and operator ID and password are shipped with the system and device identifier and secret with the console device. During initial setup, the operator enters the device identifier and associated shared secret and access password to initiate an EKE sequence between a network-attached console device and the system, as shown at block **405**. A determination is made at block **406**, whether the entered values initiates an EKE sequence. Entering correct default values establishes the first console session to the system from an authenticated device. In the preferred embodiment, only the initial console device may access the system using the default device identifier and associated shared secret. When an EKE sequence is initiated, a session secret key is generated as shown at block **407**. The result (i.e., session secret key) of the EKE sequence is utilized as a shared secret key, which replaces the initial default device shared secret as shown in block **409**. The new device shared secret is stored in protected storage on the system and is also stored as the device shared secret on the network-attached console device in a protected manner for use when the device next establishes a connection to the system as shown in block **411**.

When the network-attached console device next attempts to connect to the system, the stored device identifier and associated shared secret on the network-attached console device is utilized to complete the first EKE sequence. In one embodiment, the shared secret that is generated as part of the first EKE handshake is utilized as illustrated at block **408** to encrypt the data that will subsequently flow on the connection, namely, the authentication process for the console operator attempting to utilize a console function.

Returning to **Figure 4A**, a second EKE sequence is used to authenticate the console operator. As with the device ID, a user-id and password is also shipped with the system. The operator enters this user-id and associated password to initiate the second EKE sequence at block **413**, which initiates a second EKE sequence at block **415**. The second EKE sequence establishes a console session at the operator level as shown at block **417**. In the preferred embodiment, only the initial operator can access the machine using the default user-id. Once that initial console session is established, the operator then enters the user-id and password that is to be used for future access by the operator(s) to the console operations. The new operator user-id and password are stored on the system in protected storage at block **419**, but are not stored on the console device.

After the initial device and operator have established the initial console session with the system, the system administrator (e.g., typically the initial operator) is able to set up initial device identifiers and associated shared secrets and authorization levels for other devices the administrator desires to act as console devices as depicted at block **421**. These device identifiers and associated shared secrets and authorization levels are stored in a device table **204B** as shown at block **423**. In the preferred implementation, the system administrator also sets up initial operator user-ids and associated passwords and authorization levels for other console users to access console functions. These operator user-ids, passwords, and authorization levels are stored in the user table **204C**. The process then ends at block **425**. The stored information are illustrated in **Figures 5A** and **5B**.

Figure 5A illustrates a representative client device **501** with stored server connection information including the shared secret, i.e., hash with access password. **Figure 5B** illustrates a representative server with stored device identifier, and shared

secret, etc., in device table **511** and user identifiers and associated passwords in user table **513**.

Figure 4B illustrates one embodiment of the actual connection process after set-up of the console system as described above. Beginning at block **451**, when the operator next attempts to connect to the system by entering the access password from the authorized network-attached console device as shown at block **453**, the stored device identifier and associated shared secret on the console device are utilized for the first EKE sequence as depicted in block **455**. Then the first EKE sequence is initiated as shown at block **456**. A first determination is made at block **457** whether the first EKE sequence is successful, i.e., whether both ends of the attempted connection have identical shared secrets for the first EKE sequence. If not, access is denied (i.e., authentication process terminated) as shown at block **467**, and the process ends at block **469**. However, if both ends have identical shared secrets, then the first EKE sequence connects successfully as shown at block **459** and the shared secret is utilized to encrypt subsequent data.

Following, the operator enters the operator user-id and password at block **461** to initiate the second EKE sequence. A next determination is made at block **463** whether the second EKE sequence is successful. If the second EKE sequence is unsuccessful, then access is denied at block **467** and the process ends at block **469**. Otherwise, if the second EKE sequence is successful, then the device and operator are given access to the system's console functions as illustrated in block **465**. During operation, the operator's user-id and password are encrypted with the shared secret that is the result of the first EKE sequence. Additionally, the shared secret of the second EKE sequence is used to encrypt the data flowing over connection after the operator obtains access to the console functions as shown at block **466**.

Those skilled in the art understand that the above processes are presented as steps which are completed primarily by program code executed on the system and on the network-connected device. Different process steps may be provided and in a different order than that of **Figures 4A** and **4B**. The steps as presented are meant to illustrate only one possible representation of the invention and are not meant to be limiting on the invention in any way.

Thus, each console device may be a console for multiple machines, each server may have multiple connected console devices, and each console device may have multiple users. As described generally above, the inventions provides three main functional features, including: 1. secure device authentication; 2. dual authentication protocol using EKE; and 3. replacement of the initial device shared secret with the device session key. These features and their benefits are further explained below.

1. Secure Device Authentication

Device authentication is provided with the EKE algorithm whereby an initial shared secret is utilized and then the initial shared secret is replaced with an EKE-generated shared secret. The EKE-generated shared secret is unique to the device that generates it and unique for the system the device is being attached to. In the preferred embodiment, the shared secret generated from the EKE sequence is not provided to the operator at the console device or to any system operator. Thus, device authentication is subsequently accomplished (after the initial session) without the operator on the network-attached console device knowing the device identifier.

The method by which the device shared secret is protected on the network-attached console device is dependent on the security requirements established by the system administrator. In one embodiment, the device identifier and associated shared

secret is stored encrypted, using a key that is based on a password specified by the operator. A next, more expensive embodiment that offers more security utilizes a PC-based console device that has an embedded smart chip, which provides encrypted and physically secure storage of the device identifier.

5

The invention utilizes a network cryptographic protocol to first authenticate a physical device for console operations and then to authenticate an operator. The authentication of the physical device and subsequent authentication of the operator allows the device from which the operator completes console functions to exist anywhere in the network, without restrictions on physical connections. The only restrictions are those configured by the system administrator for the device identification and authorization level.

10

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196

sequence to authenticate the console operator. The shared secret that is generated as part of the first EKE handshake is used to encrypt and decrypt the data that will subsequently flow on the connection, i.e., the authentication process for the console operator attempting to use a console function. The secret key from the second EKE sequence is used to encrypt and decrypt session data flowing between the console device and the system.

The process ensures that the device from which the request to use console operations is made is first authenticated and that the console operator requesting console operations from that device is also authenticated, i.e., a dual authentication process. An important aspect of this dual authentication protocol using EKE is that console functions operate with a system that is in a limited functional or resource capability mode (i.e., at the beginning of installing a new operating system on the system). Using EKE and its light weight infrastructure allows the authentication with limited mode to occur.

The invention offers significant functional and usability advantages over existing solutions. The functional advantages include: (1) the system being attached to by the device can be in a limited functional mode and still be able to utilize the invention's defined protocol flow to authenticate and secure the conversations between the device and the system; (2) the novel use of EKE for device and user authentication requires fewer system resources than using a first method to authenticate the device and then another method to authenticate a user; and (3) EKE easily fits into and operates in a bootstrapped or limited system resource environment.

The third factor above is an important factor as a console must operate with a system that is in a limited resource capability. The present invention is easier to use due to the minimum configuration associated with using a protocol such as Secure

Socket Layer (SSL), which usually requires a digital certificate for each end point of the conversation, key ring support and access, and all of the associated certificate infrastructure.

3. Replacing the initial device shared secret with the device session key

The present invention utilizes a unique method to strengthen the initial network attached console device's shared secret. The method's uniqueness is that it allows a first device connection using a simple, initial genesis device identifier (shared secret) to a system from a network-attached device, to be replaced by the device session key that is negotiated from the first EKE sequence. Then the device session key of the first EKE sequence is utilized for future connections (authentication) from that specific network-attached console device. Further, the device shared secret is constantly updated each time the associated device establishes a session to the system. Thus, the initial shared secret is replaced by a much more robust and strengthened shared secret. The new strengthened shared secret is more robust because it is longer in bit length, it is more randomly generated per the EKE sequence, and it is not exposed to the operator at the network-attached device or to any other system operator.

This unique method thus magnifies the strength of the initial device shared secret. In the preferred embodiment, the new device shared secret is only known to the server and console that created it as part of the EKE flow, i.e., the new device shared secret is not known to any user or any other device. This operation will magnify the strength of the device key. There will be more entropy in the session key than in the initial shared secret that most users will use since the initial shared secret will follow password rules that users have used in the past. Thus, the initial shared secret will usually consist of 8 or less alpha numeric characters. Therefore, a 128 bit (16 byte) session key will have more entropy.

One significant benefit of the present invention is that the invention allows multiple systems, including logical partitions, to be managed from a single device. Using and relying upon the security and usability features of this invention, a device may be configured to access multiple systems and be able to use console operations on each of those systems. This eliminates the need of having one console device per system (or per logical system partition). Overall, the invention provides for greater security and integrity of the network-attached device identifier and subsequently increases the security of the system.

Finally, It is important to note that while the present invention has been described in the context of a fully functional data processing system, those skilled in the art will appreciate that the mechanism of the present invention is capable of being distributed in the form of a computer readable medium of instructions in a variety of forms, and that the present invention applies equally, regardless of the particular type of signal bearing media utilized to actually carry out the distribution. Examples of computer readable media include: nonvolatile, hard-coded type media such as Read Only Memories (ROMs) or Erasable, Electrically Programmable Read Only Memories (EEPROMs), recordable type media such as floppy disks, hard disk drives and CD-ROMs, and transmission type media such as digital and analog communication links.

While the invention has been particularly shown and described with reference to a preferred embodiment, it will be understood by those skilled in the art that various changes in form and detail may be made therein without departing from the spirit and scope of the invention.